Form FMC-15
Federal Maritime Commission
Privacy Impact Assessment (PIA)

System: ____BOX_____

Section 1. System Overview:

1.1 Describe the project/system and its purpose. (Note: this section is an overview; the questions below elicit more detail.)

Box is a FedRAMP Moderate Impact Level certified cloud-based software as a service (SaaS) platform that allows internal and external end users to store, share, and collaborate on large files safely and securely. The Federal Maritime Commission is a FIPPS 199 MODERATE environment. The security controls implemented will be based on the 800-53 R5 MODERATE designation. Box enables end users to upload up to 150 gigabytes of most file types – documents, videos, photos, etc. Box manages the hardware, software and cloud environment, and Federal Maritime Commission (FMC) manages user access and security controls for implementation of the Box platform.

Use No. 1 (Bureau of Enforcement, Investigations, and Compliance (BEIC)) – Allows BEIC to receive information related to shipping and terminal operations that is requested or required to be produced to BEIC in connection with investigation or prosecution.

Use No. 2 (Office of Equal Employment Opportunity (OEEO)) - Facilitate the secure and efficient transfer of sensitive and/or confidential personnel and other related EEO documents between key internal and external stakeholders for the purpose of adjudicating EEO actions and continuing education on EEO matters.

Section 2. Purpose and Use of the System:

2.1 Indicate legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citations/references.)

	Authority	**Citation/Reference**
	Statute	• Title VII of the Civil Rights Act of 1964 (Title VII) (Pub. L. 88-352), as amended

		• Equal Pay Act of 1963 (EPA) (Pub. L. 88-38), as amended • Pregnancy Discrimination Act (PDA) of 1978 • The Age Discrimination in Employment Act of 1967 (Pub. L. 90-202) (ADEA) • The Rehabilitation Act of 1973, as amended • Americans with Disabilities Act Amendments Act (ADAAA) • The Notification and Federal Employee Antidiscrimination and Retaliation Act (No FEAR Act) of 2002 (Pub. L. 107-174) • Elijah E. Cummings Federal Employee Antidiscrimination Act of 2020 • Genetic Information Nondiscrimination Act (GINA) of 2008 • Lilly Ledbetter Fair Pay Act of 2009 • The Pregnant Workers Fairness Act (Pub. L. 117-328) (PWFA). The PWFA is codified at 42 U.S.C. 2000gg workers Fairness Act of 2022 • 46 U.S.C. § 41302
	Executive Order	
	Federal Regulation	29 CFR § 1614 46 CFR §§ 502.281-502.291
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	

Section 3. Data Type, Sources and Use

3.1 Indicate in the table below what general categories of PII are being collected Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

General Categories of PII	
X Full Name X Date of Birth X Home Address X Phone Number(s) X Place of Birth X Age X Race/ethnicity X Alias X Sex X Email Address X Work Address X Taxpayer ID ☐ Credit Card Number X Facsimile Number X Medical Information X Education Records X Social Security Number ☐ Mother's Maiden Name ☐ Biometric Identifiers (e.g., fingerprint, voiceprint) X Audio Recordings X Photographic Identifiers (e.g., image, x-ray, video) X Certificates (e.g., birth, death, marriage, etc.) X Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.) ☐ Vehicle Identifiers (e.g., license plates) ☐ Financial Information (e.g., account number, PINs, passwords, credit report, etc.) ☐ Geolocation Information	X Passport Number ☐ User ID ☐ Internet Cookie Containing PII X Employment Status, History, or Information ☐ Employee Identification Number (EIN) X Salary X Military Status/Records/ ID Number ☐ IP/MAC Address X Investigation Report or Database X Driver's License/State ID Number (or foreign country equivalent) ☐ Other (Please Specify):

OEEO: Records include the following PII:

- Full Name - Identifies employees, former employees and applicants who contact or file complaints with the OEEO, under the statutes OEEO enforces.

- Date of Birth -Identifies date of birth for employees, former employees and applicants who contact or file complaints with the OEEO, under the Age Discrimination in Employment Act.

- Home Address - Identifies contact address for employees, former employees and applicants for the Federal Maritime Commission who contact or file complaints with the OEEO, under the statutes OEEO enforces.

- Phone Number(s) - Identifies contact numbers for employees, former employees and applicants for the Federal Maritime Commission who contact or file complaints with the OEEO, under the statutes OEEO enforces.

- Place of Birth - Identifies place of birth for employees, former employees and applicants who contact or file national origin complaints with the OEEO, under Title VII.

- Age - Identifies age of employees, former employees and applicants who contact or file complaints with the OEEO, under the Age Discrimination in Employment Act.

- Race/ethnicity - Identifies race/ethnicity of employees, former employees and applicants who contact or file race, color or national origin complaints with the OEEO, under Title VII.

- Alias - Identifies alias names of employees, former employees and applicants for the Federal Maritime Commission who contact or file complaints with the OEEO, under the statutes OEEO enforces.

- Sex - Identifies sex of employees, former employees and applicants who contact or file sex-based complaints with the OEEO, under Title VII, the PDA, the PWFA, and under the EPA.

- Email Address - Identifies contact email for employees, former employees and applicants for the Federal Maritime Commission who contact or file complaints with the OEEO, under the statutes OEEO enforces.

- Work Address - Identifies contact address for employees, former employees and applicants for the Federal Maritime Commission who contact or file complaints with the OEEO, under the statutes OEEO enforces.

- Facsimile Number - Identifies contact fax numbers for employees, former employees and applicants for the Federal Maritime Commission who contact or file complaints with the OEEO, under the statutes OEEO enforces.

- Medical Information - Identifies medical information of employees, former employees, applicants, or family members who contact or file disability or pregnancy complaints under Title VII, the Rehabilitation Act, the ADAAA, the PDA, the PWFA, or GINA, with OEEO.

- Education Records - Identifies education records of employees, former employees and applicants who contact or file non selection complaints with the OEEO, under the statutes OEEO enforces.

- Social Security Number (SSN) - Never applicable, never requested, but sometimes inadvertently provided.

- Audio Recordings - Identifies audio records obtained by OEEO during the course of investigations conducted under the statutes OEEO enforces.

- Photographic Identifiers (e.g., image, x-ray, video) Identifies video or photographic records obtained by OEEO during the course of investigations conducted under the statutes OEEO enforces.

- Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.) - Identifies legal documents, records or notes obtained by OEEO during the course of investigations conducted under the statutes OEEO enforces.

- Employment Status, History, or Information - Identifies employment history records obtained by OEEO during the course of investigations conducted under the statutes OEEO enforces.

- Salary - Identifies salary records obtained by OEEO during the course of investigations conducted under the statutes OEEO enforces.

- Military Status/Records/ ID Number - Identifies military records obtained by OEEO during the course of investigations conducted under the statutes OEEO enforces.

- Investigation Report or Database - Identifies reports of investigation, hearings and other records obtained by OEEO during the course of counseling, investigations, or hearings, conducted under the statutes OEEO enforces.

BEIC: Because of the different types of records submitted by licensed or registered entities in the shipping industry and by local, state, and federal agencies as part of BEIC's investigatory function, records transferred using Box could conceivably include almost any type of unclassified PII, including not but limited to SSN, driver's license, or passport number, for example, of the agent or regulated person or officer of a shipper or ocean transportation intermediary or terminal operator.

3.2 Provide the source(s) of the information (e.g., directly from the individual to whom the information pertains; Government (Federal, State, local, tribal); non-government sources (members of the public, public media, internet).

- Directly from the individual
- From a government database or government employee or official
- From a contract employee assigned to investigate allegations of discrimination
- From witnesses to allegations of discrimination

Section 4. Information Sharing:

4.1 What are all the Federal Maritime Commission's intended uses of the PII collected (e.g., civil enforcement, administrative matters, or human resources)?

- Administrative complaints/matters
- Human Resources and workforce analyses

4.2 Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the intended uses described above and to further the Federal Maritime Commission's mission.

The file sharing app serves OEEO by facilitating a secure and efficient transfer of sensitive and/or confidential documents between key stakeholders. This includes providing a streamlined method for delivering Reports of Investigation (ROIs), final agency decisions, settlement agreements, hearings files and other materials to and from complainants, complainant representatives, contractors, and the Office of the General Counsel (OGC) legal counsel, ensuring timely access to case materials. It also allows the OEEO to share standardized forms, templates and procedural guidance with contract and collateral duty Counselors and Investigators. Additionally, the system will support interagency and intra-agency collaboration by allowing EEO professionals to exchange best practices, policy updates, training materials, and other resources.

The file sharing application provides BEIC with the ability to receive large amounts of data in response to requests or demands related to shipping and terminal operations that is requested or required to be produced to BEIC in connection with investigation or prosecution.

4.3 With whom does the FMC intend to share the information in the system (e.g., within the agency, foreign/federal/state/local authorities, public, etc.) and how will the information be shared (e.g., case-by-case basis, bulk transfer, or direct access)?

Internal FMC staff members will be the primary users with accounts. These users will have the ability to request document uploads and to share files with other FMC staff members, other Federal Government users, State or local government users, or members of the public, on a need-to-know basis and subject to confidentiality restrictions and other restrictions required by law.

4.4 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

Information is not intended for "Open Data".

Section 5. Data Accuracy and Security:

5.1 What procedures are in place to ensure that the information is accurate, complete, and up to date?

It is the responsibility of the parties or individual submitting the data through Box to ensure the completeness, accuracy, and currency of data before submission. Additionally, data submitted through Box that is used by the FMC as part of its law enforcement, EEO policy, and other activities will be reviewed for completeness, accuracy, and timeliness in accordance with multiple factors, such as reliability of the source providing the data and FMC's business needs for the data.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system (e.g., access/security controls, monitoring/testing/evaluation, auditing, privacy training, automatic purging of information, MOUs)?

Box has a Security Categorization of FISMA Moderate. The Box SaaS has a FedRAMP authorization at the moderate Impact level. FMC has assessed and implemented all applicable security controls that are FMC's responsibility for a FISMA MODERATE baseline.

Internal users log into the Box software or Box website to upload or download files. External users upload or download files through a password-enabled Uniform Resource Locator (URL or web address) created by the internal user and shared with the external user. External users can only access the files they uploaded. Box manages the hardware, software and cloud environment, and FMC manages user access and security controls for our implementation of the Box platform.

In Box, every file is encrypted in transit with high-grade TLS encryption compliant with FIPS 140-2 standards. Once encrypted data reaches the Box network, files are 256-bit AES encrypted at rest at all times.

All FMC users and contractors must complete information security awareness training annually and privacy awareness training, or when they begin work on an FMC contract, respectively, as well as read and agree to comply with FMC's Information Technology (IT) Rules of Behavior (RoB) and Box Terms of Service prior to accessing Box.

Box is configured with automatic audit logging, which includes logging of Box Administrator activity. Further, logs are maintained separately from other system data to help ensure compliance with tiered/role-based access as well as to help safeguard against unauthorized access, use, and disclosure of information. Box audit logs can only be accessed in read-only mode by authorized FMC's Box Administrator who has privileged access. Box audit logs are automatically monitored by the Box Security Incident and Event Management (SIEM) tool,. FMC's Box Administrator has exclusive access to the audit logs.

Section 6. Data Retention and Disposal

6.1 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. Reference the applicable retention schedule approved by the National Archives and Records Administration, if available or necessary.

Box is used only as a transport infrastructure and is not designed as an official record-keeping system, document archival system, or document backup system. Offices will develop a Standard Operating Procedure (SOP) to transfer files from Box to Sharepoint or other official record-keeping system with established timelines and to manually delete files after transferring. This retention period is consistent with NARA GRS 5.2: Intermediary Records, which states that the records are temporary and must be destroyed upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

Box metadata is considered non-intermediary records, and is automatically accessible within the Box platform by FMC administrator in the form of user activity report (i.e, log of all file activity) kept for 7 years. User activity report (i.e, log of all file activity) is kept for 7 years, and FMC administrator for Box can run the customizable report by selecting the date range and the filters sought for in the report, such as download date, upload date, user name, affected file name, among other things. This retention period for metadata is consistent with NARA GRS 3.1 051, which states that the records are temporary and can be destroyed 5 years after the project/activity/transaction is completed or superseded, or the associated system is terminated, or the associated data is migrated to a successor system, but longer retention is authorized if required for business use.

Section 7. Notice, Consent, and Redress:

7.1 Will individuals be notified if their information is collected, maintained, or disseminated by the system (e.g., system of records notice, Privacy Act 552a(e)(3) notice)? Please specify. If no notice is provided, please explain.

Typically no, because individuals knowingly provide the information via the link to the FMC Box.com account, so notice is therefore not necessary. When required, the FMC provides notice to individuals about its policies regarding the use and disclosure of information at the time information is collected (e.g., in voluntary access letters, civil investigatory demands, or agency forms or questionnaires that were originally used to request or collect the information uploaded to the system). Box also contains an appropriate Privacy Notice.

7.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system. For example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Opportunities to consent to collection or specific uses of their information depend on the business use of the information. For non-mandatory information, individuals may decline to provide the information requested by FMC. For mandatory information where the uses of information are not subject to the consent of the individual providing the information (e.g., information provided pursuant to a court order or subpoena), individuals do not have any opportunity to decline to provide the information or to consent to particular uses of the information.

7.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Box is used only as a transport infrastructure and so does not meet the requirements of a Privacy Act System of Records. Documents and files sent to the FMC through Box are incorporated into FMC's Sharepoint database. OEEO records, to the extent such records are retrieved by personal identifier, are covered by existing System of Records Notice (SORN), FMC-28 (EEOC/GOVT-1), available at 78 Fed. Reg. 55703 (Sept. 11, 2013). Requests to amend or correct such OEEO records can be submitted by following the instruction in the SORN. For BEIC records received through Box, there is no procedure to request to amend or correct records, because BEIC records do not meet the requirements of a Privacy Act System of Records. Specifically, BEIC records are not "about" an individual. Additionally, although records may include PII incidentally stored, such as name and phone number of primary point of contact, the use is ancillary to the FMC's enforcement, regulatory, and other activities. Moreover, BEIC does not as a general and routine practice index or retrieve records about an individual using a personal identifier assigned to that individual.

Section 8. Website Privacy Evaluation

8.1 Does the project/system employ the use of a website or application?

Yes. Box.com

8.2 If so, describe any tracking technology used by the website or application and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

Box may collect personal identifiers from the users automatically. These identifiers include IP address, device identifiers, advertising ID and other information about user's browser or device. Box may collect this information via cookies and other tracking technologies and use it to enhance, customize, improve and notify the user about their Services.

8.3 Does the project/system employ the use of a third-party website or application?

Yes. Box.com

8.4 If so, include: i. the specific purpose of the agency's use of the third-party website or application; ii. any PII that is likely to become available to the agency through public use of the third-party website or application; iii. the agency's intended or expected use of PII; iv. with whom the agency will share PII; v. whether and how the agency will maintain PII, and for how long; vi. how the agency will secure PII that it uses or maintains; vii. what other privacy risks exist and how the agency will mitigate those risks; and viii. whether the agency's activities will create or modify a "system of records" under the Privacy Act. (This may be done as a separate PIA.)

Parts i though vi, and Part viii are answered in the above Sections 1 through 6. Regarding the remaining Part vii about identifying privacy risks and mitigating such risks, please see below.

Risk	Mitigation Strategy
Users could exceed their authorized access and view documents or files from other accounts.	System administrators do not have access to the files uploaded to Box. Administrators can only view a list of the files being transferred and stored, and can only delete, replicate, and set life cycle rules for each file if necessary. FMC users can only access their own files, or files explicitly shared to them. They cannot access files provided to other FMC users unless that user shares the file with them.
A user (whether within the FMC or outside) could upload infected or malicious files and compromise the security of the system.	To address this risk, files uploaded to Box are scanned for viruses, and files found to be infected are rejected. The Box anti-virus software receives daily updates to active virus signatures. The FMC recognizes that, despite these precautions, zero-day viruses (defined as a previously unknown virus for which specific anti-virus software signatures are not yet available) remain possible threats.

Section 9. Privacy Act Compliance:

9.1 Is a Privacy System of Records being developed or modified for this System? If so, provide the status or link to the System of Record Notice published in the Federal Register below:

No, because Box is used only as a transport infrastructure and so does not meet the requirements of a Privacy Act System of Records.